

REMARKS/ARGUMENTS

Reconsideration of this application is respectfully requested.

The Examiner is thanked for including explanatory comments with the advisory action of May 23, 2008. The above amendments and the following comments are an attempt to further respond to the last (final) office action and to the Examiner's remarks set forth in the advisory action.

Applicant's earlier stated traversals of all outstanding grounds of rejection are hereby repeated and incorporated by reference.

The applicant's claimed invention analyzes traffic log data as a function of a pre-determined traffic characteristic criterion so as to identify electronic messages that satisfy that traffic characteristic criterion. Various actions can be taken with respect to such identified electronic messages.

In addition, the applicant's claimed invention utilizes at least one server interposed between the message originator and the message recipient. Corrective action may then be taken within that intermediate server and/or other intermediate servers, if needed.

By contrast, Hile teaches a direct source-to-destination communication link. A portion of the destination RAM 20 is allocated to an input buffer for incoming messages/data and, before such is transferred to another area of RAM for use, it is

scanned to see if it contains known virus strings. If some known virus string within the content of the message is discovered, then corrective action may be initiated (e.g., preventing that message from ever being transferred to any other part of the RAM 20).

The Examiner asserts that Hile:

“...identifies the destination of the data being transmitted...” [Page 2 of advisory action, lines 1-2.]

While it is, of course, common practice for messages to include a header identifying a destination, Hile does not actually teach this conventional aspect of message communication. Not surprisingly, Hile does not teach any process that is performed as a function of such destination identity data.

The Examiner also asserts:

“...depending on the analyzed transmitted data between the computer systems and the data characters such as size of the data or the destination of the data, the data transmission could be suspended.” [Page 2 of advisory action, lines 3-4.]

Actually, Hile does not teach any testing of an incoming message based on size of the data or destination of the data. The only testing by Hile with respect to “data characters” is to look for known virus strings that are stored in finite state tables 34. Whatever action is taken by Hile is necessarily a function only of the content of the incoming message itself – not a function of any traffic log data.

The Examiner asserts differently by stating:

“So, this data is log data because it contains characters as shown in Fig. 3 which are traffic characteristics, and by using Sorkin et al. that teaches log data and also teaches a system and method for analyzing log files, wherein the log files are log data as mentioned in the applicant’s claims.” [Advisory action, page 2, lines 5-7.]

While it is true that Fig. 3 in Hile (in conjunction with Figs. 4 and 5) teaches an exemplary search for a virus string comprising any of the three words “tale,” “tool” and “ale,” these are merely known virus signature strings that are being searched for within the message itself. They are not traffic characteristics in any rational sense of that term – nor are they described as such anywhere in Hile. Nor does Sorkin teach maintaining or analyzing any traffic log files based on at least one traffic characteristic derived from handling of plural electronic messages. Instead, Sorkin (discussed in more detail below) only reviews log files of hacker intrusion actions within a given machine – not traffic characteristics associated with handling of plural electronic messages.

Clearly, the virus string signature characters depicted in Fig. 3 cannot be “traffic characteristics” of any sort. Instead, they are merely character strings known *a priori* to be associated with a virus – totally irrespective of any traffic log data.

Neither Hile nor Sorkin even mentions use of a traffic log file as recited in the applicant’s claims.

The Examiner's further comments about Fig. 2 of Hile are perhaps not completely understood:

"Also, in Fig. 2, if the user wishes to copy or send data from a first computer to a second computer, it is assumed that the first user is not secure or has corrupt data then the data is not sent or copied by suspending the delivery of the data." [Advisory action, page 2, lines 8-9.]

The Hile teaching does not have any apparent mechanism for preventing data from being sent from a first user – even if that first user is known to be insecure, etc. Instead, the Hile teaching does not interpose a server between the source and destination. Rather, the Hile teaching depends entirely upon analyzing what has already been received at the destination – albeit initially segregated into a buffer area 30 of RAM 20. Hile can only suspend the "delivery" of data if the destination machine detects a virus string to be present and then refuses to pass the data onward from the buffer area 30 of RAM 20. This is a teaching directly contrary to the applicant's claimed arrangement where there is at least one server interposed between the source and destination of messages.

The Examiner may not fully appreciate the fact that there is no intermediate server between the source and destination in Hile because the Examiner states as follows:

"Regarding the data being tested between the computer systems, Hile teaches testing data between two computer systems which could be a file, e-mail, or a message." [Advisory action, page 2, lines 10-11.]

It is self-evident from Hile (e.g., see Fig. 1) that there is nothing interposed between the modems 28 attaching the source to the destination. Furthermore, as indicated in both figures and the text, the input buffer 30 is merely a portion of RAM 20 already located at the destination. See, for example, 3:64-67 and the associated dotted lines in the various figures of Hile. There is no interposed server or other mechanism in Hile located between different computer systems. Hile merely teaches conventional virus detection by analyzing the input buffer of the destination for a known virus string before permitting the content of the sequestered input buffer to be further utilized or transferred to other portions of the destination memory.

The Examiner has also asserted that the applicant's claims have failed to sufficiently recite certain previously argued features – namely, the testing of traffic log data as a function of traffic characteristics associated with incoming data. In response, the claims have been amended above so as to make that requirement more explicit.

It seems that the Examiner considers that merely because Hile analyzes transmitted data (the content of an e-mail, for example), and because a decision to suspend the use of such data (or not) is made in dependence on the analysis (i.e., in dependence on whether a virus string is found), then this data itself is “traffic log” data. In view of the Examiner's reference to Fig. 3 of Hile, it seems that he also may be considering the virus

itself to be "traffic log" data on the basis that it determines the future use of the data. Either possibility is incorrect.

Clearly, the characters shown in Hile's Fig.3 cannot be said to be traffic characteristics since they do not, in themselves, provide any information about traffic. They merely provide information which may, but need not, be subsequently used to make a data delivery (traffic) decision. Until the message data itself is used to make such a decision, it cannot give rise to even generating traffic data. That is, the Fig. 3 data cannot be used to make a delivery decision until it has been analyzed. Hence, what is analyzed cannot itself be said to already be traffic data (let alone traffic log data).

It is, therefore, impermissible to construe the phrase "log data relating to one or more traffic characteristics associated with electronic messages" as including information merely contained within a given message even if this information is used as a factor in a subsequent traffic-related (e.g., delivery) decision. It is clear that this phrase in the applicant's claims is directed to the characteristics of the actual flow of plural messages rather than the information contained within a given single message. Furthermore, the construction apparently placed upon this phrase by the Examiner ignores the common meaning of the word "log," which requires a chronological record of events and, therefore, not just a single virus signature (supplied *a priori* as known to be a virus string by means not depicted in Hile) as suggested by the Examiner.

Paul W. HODGSON
Serial No. 10/522,919
July 7, 2008

Perhaps the Examiner considers "traffic log data" could be found in Hile in the form of a record indicating that a virus has been previously found, this record being the particular state of the finite state machine referred to by the Examiner in Fig.3. If this is the case, the analyzing means of claim 1 can no longer be said to be the means that scan for virus signatures inasmuch as this would imply that the traffic log data is analyzed before it is created.

The Examiner also appears to have shifted position since the final office action, where it was stated that "log data was not taught in Hile," but that it was taught in Sorkin. Now, the Examiner asserts that log data is taught in Hile. Conversely, the step of analyzing this log data is now said by the Examiner to be taught by Sorkin, whereas in the final office action, the step of analyzing the data was asserted to be taught by Hile.

In fact, neither Hile nor Sorkin teaches use of traffic log data to make protective decisions in a message handling environment.

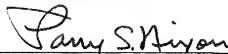
Paul W. HODGSON
Serial No. 10/522,919
July 7, 2008

Accordingly, it is believed that this entire application is now in condition for allowance, and a formal notice to that effect is respectfully solicited.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By:

A handwritten signature in dark ink, appearing to read "Larry S. Nixon", is written over a horizontal line.

Larry S. Nixon
Reg. No. 25,640

LSN:lef

901 North Glebe Road, 11th Floor
Arlington, VA 22203-1808
Telephone: (703) 816-4000
Facsimile: (703) 816-4100